

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of : Daniel Timmermans
For : PROTECTION AGAINST POWER
: ANALYSIS ATTACKS
Serial No. : 10/587,727
Filed : July 26, 2006
Art Unit : 2431
Examiner : Zia, Syed
Att. Docket No. : NL040060US1
Confirmation No. : 1413

APPEAL BRIEF

Mail Stop Appeal Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Customer No.

65913

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed July 30, 2010.

I. REAL PARTY IN INTEREST

The party in interest is NXP B.V., by way of an Assignment recorded at Reel 019719, Frame 0843.

II. RELATED APPEALS AND INTERFERENCES

Following are identified any prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal:

NONE.

III. STATUS OF CLAIMS

Claims 1-8 and 10-16 are on appeal.

Claims 1-8 and 10-22 are pending.

Claims 1-8 and 10-16 are rejected.

Claim 9 is canceled.

Claims 17-22 are objected to.

IV. STATUS OF AMENDMENTS

All Amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites "an electronic circuit for cryptographic processing, comprising: a first combinatorial logical circuit [Fig. 1: 101], having an input, arranged

to perform a first set of logical operations on an input data [Fig. 1: 129] at the input and to produce a corresponding first output data [Fig. 1: 119], the first output data [Fig. 1: 119] having a first functional relation to the input data [Fig. 1: 129] for said input data [Fig. 1: 129] within a given range, and a second combinatorial logical circuit [Fig. 1: 103], having an input, arranged to perform a second set of logical operations on an input data [Fig. 1: 129] at said input and to produce a corresponding second output data [Fig. 1: 121], the second output data [Fig. 1: 121] having a second functional relation to the input data [Fig. 129:], said second functional relation identical to said first functional relation for said input data [Fig. 1: 129] within said given range, wherein the first set of logical operations is different from the second set of logical operations, and a selector [Fig. 1: 111] for receiving a given input data and dynamically selecting from among the first combinatorial logical circuit [Fig. 1: 101] for performing the first set of logical operations on the given input data and the second combinatorial logical circuit [Fig. 1: 103] for performing the second set of logical operations on the given input data [and producing output data [Fig. 1: 131], and wherein the selecting includes inputting the given input data to the input of the selected one of the first [Fig. 1: 101] and second [Fig. 1: 103] combinatorial logical circuits and outputting a selected first cryptographic processing output [Fig. 1: 131], the selected first cryptographic processing output [Fig. 1: 131] being the output of the selected one of the first [Fig. 1: 101] and second [Fig. 1: 103] combinatorial logical circuits.”

Independent claim 5 recites: “An electronic circuit for cryptographic processing, comprising: a combinatorial logical circuit to perform logical operations on input data and to produce an output data, a storage circuit for storing the output data produced by the combinatorial logical circuit, wherein the storage circuit comprises a first encoding means [Fig. 4: 403] for encoding the output data into a first encoded output data [Fig. 4: 427], a storage element [Fig. 4: 401] for retrievably storing the first encoded output data [Fig. 4: 427], a corresponding first decoding means [Fig. 4: 405], arranged for decoding the first encoded output data [Fig. 4: 427] into said output data [Fig. 4: 431] after retrieving the first encoded output data [Fig. 4: 427] from the storage element [Fig. 4: 401], and wherein the electronic circuit is arranged to dynamically control the activation of the first encoding means [Fig. 4: 403] and the corresponding first decoding means [Fig. 4: 405].”

Independent claim 10 recites: “A method of processing cryptographic data, comprising: using a set of logical operations for processing input data and producing output data, storing the output data in a storage element, wherein the storing comprises: encoding [Fig. 4: 403] the output data into an encoded output data [Fig. 4: 427], storing the encoded output data [Fig. 4: 427] in the storage element [Fig. 4: 401], retrieving the encoded output data [Fig. 4: 427] from the storage element [Fig. 4: 401], decoding [Fig. 4: 405] the encoded output data [Fig. 4: 427] retrieved from the storage element [Fig. 4: 401], and dynamically controlling the encoding [Fig. 4: 403] of the

output data into an encoded output data [Fig. 4: 427] and the corresponding decoding [Fig. 4: 405] of the encoded output data [Fig. 4: 427] retrieved from the storage element [Fig. 4: 401].”

Independent claim 16 recites: “A method of processing cryptographic data, comprising: generating a mode signal having one of a given plurality of states; receiving a given input data and generating a cryptographic processed data output, said generating including: generating a first input data, wherein the first input data is a selected one of a mask of the given input data and a not mask of the given data, the selection based on the state of the mode signal; generating a second input data, wherein the second input data is the other of the mask of the given input data and the not mask of the given data, performing a first set of logical operations [Fig. 3: 319] on the first input data to generate a first output data, the first set of logical operations [Fig. 3: 319] embodying a given input-output function, performing a second set of logical operations [Fig. 3: 321] on the second input data to generate a second output data, the second set of logical operations [Fig. 3: 321] being different than the first set of logical operations [Fig. 3: 319] and the second set of logical operations [Fig. 3: 321] embodying the same given input-output function, and merging [Fig. 3: 317] the first output data and the second output data to generate the cryptographic data output [Fig. 3: 333]; repeating said generating a mode signal to have a different one of the given plurality of states; and repeating said receiving a given input data and generating a cryptographic

processed data output.”

Dependent claim 2 recites: “a third combinatorial logical circuit [Fig. 5: 511], having an input, arranged to perform a third set of logical operations on an input data [Fig. 5: 569] at said input and to produce a corresponding third output data, the third output data having a third given functional relation to said input data [Fig. 5: 569] for input data [Fig. 5: 569] within a given range, and a fourth combinatorial logical circuit [Fig. 5: 513], having an input, arranged to perform a fourth set of logical operations on an input data [Fig. 5: 569] at said input and to produce a corresponding fourth output data, the fourth output data having a fourth functional relation to said input data [Fig. 5: 569] identical to said given third functional relation, wherein the third set of logical operations is different from the fourth set of logical operations, and a selector [Fig. 5: 563] for receiving said selected first cryptographic processing output data and dynamically selecting from among the third combinatorial logical circuit [Fig. 5: 511] and the fourth combinatorial logical circuit [Fig. 5: 513] for performing logical operations on the selected first cryptographic processing output data and producing a second output cryptographic processing data, and wherein said selecting includes inputting the selected first cryptographic processing output data to the input of the selected one of the third [Fig. 5: 511] and fourth [Fig. 5: 513] combinatorial logical circuits.”

Dependent claim 3 recites: “a selection circuit [Fig. 5: 563] for generating a

selecting signal to select one combinatorial logical circuit from among the first [Fig. 5: 507] and second [Fig. 5: 509] combinatorial logical circuits, a splitter circuit [Fig. 5: 543] for inputting the given input data [Fig. 5: 569] to one of the first [Fig. 5: 507] and second [Fig. 5: 509] combinatorial logical circuits, depending on the selecting signal, a merger circuit [Fig. 5: 553] for outputting data from one of the first [Fig. 5: 507] and second [Fig. 5: 509] combinatorial logical circuits, depending on the selecting signal.”

Dependent claim 4 recites: “a timing circuit [Fig. 4: 423] to determine the points in time at which the selection circuit [Fig. 4: 421] generates the selecting signal to select one of the first [Fig. 4: 403] and second [Fig. 4: 407] combinatorial logical combinatorial logical circuits.”

Dependent claim 6 recites: “a second encoding means [Fig. 4: 407] for encoding the output data into a second encoded output data for storing in the storage element [Fig. 4: 401], a corresponding second decoding means [Fig. 4: 409], arranged for decoding the second encoded output data into said output data after retrieving the second encoded output data from the storage element [Fig. 4: 401], wherein the encoding of the first output data is different from the encoding of the second output data, and wherein the electronic circuit is further arranged to generate a selecting signal to dynamically select from among the first encoding means [Fig. 4: 403] and its corresponding first decoding means [Fig. 4: 405] and the second encoding means [Fig. 4: 407] and its corresponding second decoding means [Fig. 4: 409], for encoding and

decoding of the output data.”

Dependent claim 7 recites: “a timing circuit [Fig. 4: 423] to determine the points in time at which the electronic circuit selects one from among the first [Fig. 4: 403] and second [Fig. 4: 407] encoding means and corresponding first [Fig. 4: 405] and second [Fig. 4: 409] decoding means.”

Dependent claim 12 recites: “a first mask circuit [Fig. 1: 113] for selectively masking and not masking, based on the signal, the given input data [Fig. 1: 129] for input to the first combinatorial logical circuit [Fig. 1: 101], and a second mask circuit [Fig. 1: 115] for selectively masking and not masking, based on the signal, the given input data [Fig. 1: 129] for input to the second combinatorial logical circuit [Fig. 1: 103].”

Dependent claim 13 recites: “a first mask circuit [Fig. 1: 113] to selectively mask and not mask, based on the signal, the given input data [Fig. 1: 129] and to input the selected masked and not masked given input data to the first combinatorial logical circuit [Fig. 1: 101], and a second mask circuit [Fig. 1: 115] to selectively mask and not mask, based on the signal, to input the selected masked and not masked given input data [Fig. 1: 129] to the second combinatorial logical circuit [Fig. 1: 103].”

Dependent claim 15 recites: “wherein the selector [Fig. 1: 111] includes an OR merger circuit [Fig. 1: 109] to receive the output of the first combinatorial logical circuit [Fig. 1: 101] and to receive the output of the second combinatorial logic circuit [Fig. 1:

103], and to output, as the selected output [Fig. 1: 131], a logical OR of the output of the first combinatorial logical circuit [Fig. 1: 101] and the output of the second combinatorial logic circuit [Fig. 1: 103]."

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are presented for review:

A. On pages 4-9, the final Office Action rejects claims 1-8 and 10-16 under 35 U.S.C. § 102(e) as allegedly anticipated by Pub. No. US2005/0089060 to Vergnes (“Vergnes”).

VII. ARGUMENT

A. Rejection of Claims 1-8 and 10-16 Under 35 U.S.C. § 102(e)

The final Office Action dated April 30, 2010, rejects claims 1-8 and 10-16 under 35 U.S.C. § 102(e) as allegedly anticipated by Vergnes.

The test for anticipation under section 102 is whether each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); MPEP §2131. The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989); MPEP §2131. The elements must also be arranged as required by the claim. *In re Bond*, 15 USPQ2d 1566 (Fed. Cir. 1990).

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). Here, Appellant respectfully submits that Vergnes fails to provide "each and every element" recited by the claims.

1. Independent Claims 1, 5, and 8

Independent claim 1 recites "a first combinatorial logical circuit," "a second combinatorial logical circuit," and "a selector" (emphasis added). Similar subject matter appears in claims 5 and 8. Appellant respectfully submits that Vergnes fails to

disclose, suggest, or teach this subject matter.

The Office Action fails to directly address any of this subject matter, instead listing a series of figure and paragraph numbers from Vergnes without any further explanation. No details are provided, so the Office Action clearly does not show the identical invention in as complete detail as is contained in the claim. Thus, the Office Action fails to comply with the anticipation standard for 35 U.S.C. § 102(e).

Second, the Office Action ignores the recited subject matter of having “the first set of logical operations is different from the second set of logical operations.” Even if Vergnes has “combinatorial circuits 412,” there is no disclosure in Vergnes that these circuits have different logical operations.

Third, Vergnes does not have first and second combinationorial circuits operating in parallel on the same input data. Instead, the combinatorial circuits of Vergnes are arranged in series, with combinatorial circuit 412-2 receiving manipulated input from combinatorial circuit 412-1. See paragraph [0033] of Vergnes. Because these combinatorial circuits are arranged in series instead of in parallel, a selector could not function on these circuits in the recited manner.

2. Independent Claim 10

Independent claim 10 recites “dynamically controlling the encoding of the output data into an encoded output data and the corresponding decoding of the encoded output data retrieved from the storage element” (emphasis added). Appellant respectfully

submits that Vergnes fails to disclose, suggest, or teach this subject matter.

For a proper anticipatory rejection, “the elements must be arranged as required by the claim.” *In re Bond*, 910 F.2d 831 (Fed. Cir. 1990). Here, the Office Action fails to directly address any of this subject matter, instead listing a series of figure and paragraph numbers from Vergnes without any further explanation. No details are provided, so the Office Action fails to comply with the anticipation standard for 35 U.S.C. § 102(e), as described above for the other independent claims.

3. Independent Claim 16

Independent claim 16 recites “generating a first input data, wherein the first input data is a selected one of a mask of the given input data and a not mask of the given data, the selection based on the state of the mode signal” (emphasis added). Appellant respectfully submits that Vergnes fails to disclose, suggest, or teach this subject matter.

For a prima facie rejection based upon 35 U.S.C. § 102, “all words in a claim must be considered in judging the patentability of a claim against the prior art.” *In re Wilson*, 424 F.2d 1382 (C.C.P.A. 1970). In this case, Appellant respectfully submits that Office Action fails to consider any of the words in claims 1, 5, 10, and 16, but instead rejects all of these claims in the same way, alleging that they are somehow anticipated by out-of-context excerpts of figure and paragraph numbers from Vergnes.

On page 3, the Office Action alleges that “cited prior art does teach or suggest

the subject matter recited in independent and dependent claims” but fails to actually address that subject matter. Instead, the Office Action yet again refers to (Fig. 4-6 and [0031-0036, 0046-0047, and 0051]), out-of-context figure and paragraph numbers from Vergnes that fail to provide any detail regarding the recited claims. Moreover, page 3 of the Office Action also refers to the language taken from the Abstract of Vergnes but completely fails to provide any explanation as to why this language should be applicable to any of the claims.

For the reasons listed above, Appellant respectfully submits that independent claims 1, 5, 10, and 16 are allowable over the references of record.

4. Dependent Claim 2

According to MPEP § 2111.01, “the words of the claim must be given their plain meaning unless the plain meaning is inconsistent with the specification.” In this case, Appellant respectfully submits that the current Office Action has clearly misinterpreted the words of claim 2. While claim 2 actually recites “a third combinatorial logical circuit” and “a fourth combinatorial logical circuit,” page 6 of the Office Action refers to a “first set” and a “second set” of combinatorial logic circuits. Such language simply does not appear in the current version of claim 2.

5. Dependent Claim 3

Dependent claim 3 recites “a selection circuit,” “a splitter circuit,” and “a merger circuit” (emphasis added). Appellant respectfully submits that Vergnes fails to

disclose, suggest, or teach this subject matter.

On page 7, the Office Action alleges that Fig. 4 of Vergnes somehow anticipates this subject matter. In response, Fig. 4 discloses neither a selection circuit nor a splitter circuit nor a merger circuit. Further, the Office Action provides no explanation as to why paragraphs [0034-0036] and [0046-0047] in Vergnes are germane to this claim language.

6. Dependent Claims 4 and 7

Dependent claims 4 and 7 recite “a **timing** circuit” (emphasis added). Appellant respectfully submits that Vergnes fails to disclose, suggest, or teach this subject matter.

Pages 7 and 8 of the Office Action are inconsistent with respect to this subject matter. While page 7 alleges that Figs. 4-6 and paragraphs [0046-0048] somehow anticipate claim 4, page 8 relies upon Fig. 5 and paragraphs [0046-0049]. No explanation of this discrepancy appears in the Office Action.

7. Dependent Claims 12 and 13

Dependent claims 12 and 13 recite “a **first mask** circuit” and “a **second mask** circuit” (emphasis added). Appellant respectfully submits that Vergnes fails to disclose, suggest, or teach this subject matter.

Pages 8 and 9 of the Office Action completely fail to address this subject matter. Exactly the same figure and paragraph numbers are cited as for the independent

claims. No explanation appears regarding any interpretation of the disclosure of Vergnes relative to the recited mask circuits.

8. Dependent Claim 15

Dependent claim 15 recites “an **OR merger** circuit” in the context of a selector (emphasis added). Appellant respectfully submits that Vergnes fails to disclose, suggest, or teach this subject matter.

Page 9 of the Office Action also fails to address the subject matter of claim 15. As for the previous claims, it merely repeats the figure and paragraph numbers cited for the independent claims. There is no analysis of the actual claim language.

9. Summary

Also, claims 2-4, 11, 12, and 15 depend from claim 1. Claims 6-8, 13, and 14 depend from claim 5. Thus claims 2-4, 6-8, and 11-15 are also allowable at least due to their respective dependencies from allowable claims. Thus, Appellant respectfully requests withdrawal of all pending rejections under 35 U.S.C. § 103(a).

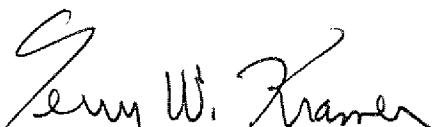
CONCLUSION

For at least the reasons discussed above, it is respectfully submitted that the rejections are in error and that claims 1-8 and 10-16 are in condition for allowance. For at least the above reasons, Appellants respectfully request that this Honorable Board reverse the rejections of claims 1-8 and 10-16.

In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account. Should there be any remaining issues that could be readily addressed over the telephone; the Examiner is asked to contact the attorney overseeing the application file, Juergen Krause-Polstorff, of NXP Corporation at (408) 474-9062.

Respectfully submitted,
KRAMER & AMADO, P.C.

Date: July 30, 2010



Terry W. Kramer
Reg. No. 41,541

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131
CUSTOMER NO.: 65913

VIII. CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL:

1. (Rejected) An electronic circuit for cryptographic processing, comprising:
 2. a first combinatorial logical circuit, having an input, arranged to perform a first set of logical operations on an input data at the input and to produce a corresponding first output data, the first output data having a first functional relation to the input data for said input data within a given range, and
 6. a second combinatorial logical circuit, having an input, arranged to perform a second set of logical operations on an input data at said input and to produce a corresponding second output data, the second output data having a second functional relation to the input data, said second functional relation identical to said first functional relation for said input data within said given range,
 11. wherein the first set of logical operations is different from the second set of logical operations, and
 13. a selector for receiving a given input data and dynamically selecting from among the first combinatorial logical circuit for performing the first set of logical operations on the given input data and the second combinatorial logical circuit for performing the second set of logical operations on the given input data and producing output data, and
 17. wherein the selecting includes inputting the given input data to the input of the

18 selected one of the first and second combinatorial logical circuits and outputting a
19 selected first cryptographic processing output, the selected first cryptographic
20 processing output being the output of the selected one of the first and second
21 combinatorial logical circuits.

1

1 2. (Rejected) The electronic circuit of claim 1, further comprising:

2 a third combinatorial logical circuit, having an input, arranged to perform a
3 third set of logical operations on an input data at said input and to produce a
4 corresponding third output data, the third output data having a third given functional
5 relation to said input data for input data within a given range, and

6 a fourth combinatorial logical circuit, having an input, arranged to perform a
7 fourth set of logical operations on an input data at said input and to produce a
8 corresponding fourth output data, the fourth output data having a fourth functional
9 relation to said input data identical to said given third functional relation,

10 wherein the third set of logical operations is different from the fourth set of
11 logical operations, and

12 a selector for receiving said selected first cryptographic processing output data
13 and dynamically selecting from among the third combinatorial logical circuit and the
14 fourth combinatorial logical circuit for performing logical operations on the selected
15 first cryptographic processing output data and producing a second output cryptographic

16 processing data, and

17 wherein said selecting includes inputting the selected first cryptographic
18 processing output data to the input of the selected one of the third and fourth
19 combinatorial logical circuits.

1

1 3. (Rejected) The electronic circuit of claim 1, wherein the selector comprises:

2 a selection circuit for generating a selecting signal to select one combinatorial
3 logical circuit from among the first and second combinatorial logical circuits,

4 a splitter circuit for inputting the given input data to one of the first and second
5 combinatorial logical circuits, depending on the selecting signal,

6 a merger circuit for outputting data from one of the first and second
7 combinatorial logical circuits, depending on the selecting signal.

1

1 4. (Rejected) The electronic circuit of claim 3, further comprising:

2 a timing circuit to determine the points in time at which the selection circuit
3 generates the selecting signal to select one of the first and second combinatorial logical
4 combinatorial logical circuits.

1

1 5. (Rejected) An electronic circuit for cryptographic processing, comprising:

2 a combinatorial logical circuit to perform logical operations on input data and to

3 produce an output data,
4 a storage circuit for storing the output data produced by the combinatorial logical
5 circuit,
6 wherein the storage circuit comprises
7 a first encoding means for encoding the output data into a first encoded output
8 data,
9 a storage element for retrievably storing the first encoded output data,
10 a corresponding first decoding means, arranged for decoding the first encoded
11 output data into said output data after retrieving the first encoded output data from
12 the storage element, and
13 wherein the electronic circuit is arranged to dynamically control the activation of
14 the first encoding means and the corresponding first decoding means.

1
1 6. (Rejected) The electronic circuit of claim 5, wherein the storage circuit further
2 comprises:

3 a second encoding means for encoding the output data into a second encoded
4 output data for storing in the storage element,
5 a corresponding second decoding means, arranged for decoding the second
6 encoded output data into said output data after retrieving the second encoded output
7 data from the storage element,

8 wherein the encoding of the first output data is different from the encoding of the
9 second output data, and

10 wherein the electronic circuit is further arranged to generate a selecting signal to
11 dynamically select from among the first encoding means and its corresponding first
12 decoding means and the second encoding means and its corresponding second decoding
13 means, for encoding and decoding of the output data.

1
1 7. (Rejected) The electronic circuit of claim 6, further comprising:
2 a timing circuit to determine the points in time at which the electronic circuit
3 selects one from among the first and second encoding means and corresponding first
4 and second decoding means.

1
1 8. (Rejected) The electronic circuit of claim 6, wherein the combinatorial logical circuit
2 comprises:

3 a first combinatorial logical circuit, having an input, arranged to perform a first
4 set of logical operations on input data at the input and to produce a corresponding first
5 cryptographic output data, the first cryptographic output data having a given first
6 functional relation to the input data for said input data within a given range, and

7 a second combinatorial logical circuit, having an input, arranged to perform a
8 second set of logical operations on input data at said input and to produce a

9 corresponding second cryptographic output data, the second cryptographic output data
10 having a functional relation to the input data identical to the given first functional
11 relation for said input data within said given range,

12 wherein the first set of logical operations is different from the second set of
13 logical operations, and

14 a selector for receiving an input data and dynamically selecting from among the
15 first combinatorial logical circuit and the second combinatorial logical circuit for
16 performing logical operations on the given input data and producing output data, and

17 wherein the selecting includes inputting the input data to the input of the
18 selected one of the first and second combinatorial logical circuits and outputting a
19 selected output, the selected output being the output of the selected one of the first and
20 second combinatorial logical circuits.

1
9. (Canceled).

1
1 10. (Rejected) A method of processing cryptographic data, comprising:
2 using a set of logical operations for processing input data and producing output
3 data,
4 storing the output data in a storage element, wherein the storing comprises:
5 encoding the output data into an encoded output data,

1

1 11. (Rejected) A cryptographic device comprising an electronic circuit according to claim
2 1.

1

12. (Rejected) The electronic circuit of claim 1, wherein the selector includes:

- 2 a first mask circuit for selectively masking and not masking, based on the signal,
- 3 the given input data for input to the first combinatorial logical circuit, and
- 4 a second mask circuit for selectively masking and not masking, based on the
- 5 signal, the given input data for input to the second combinatorial logical circuit.

1

13. (Rejected) The electronic circuit of claim 8, wherein the selector includes:

2 a first mask circuit to selectively mask and not mask, based on the signal, the
3 given input data and to input the selected masked and not masked given input data to
4 the first combinatorial logical circuit, and

5 a second mask circuit to selectively mask and not mask, based on the signal, to
6 input the selected masked and not masked given input data to the second combinatorial
7 logical circuit.

1

1 14. (Rejected) The electronic circuit of claim 13,

2 wherein the first mask circuit includes an AND mask configured to mask and to
3 not mask the given input data by inputting to the first combinatorial logical circuit a
4 selection between all zeros and the given input data, respectively and

5 wherein the second mask circuit includes an AND mask configured to mask and
6 to not mask the given input data by inputting to the second combinatorial logical
7 circuit a selection between all zeros and the given input data, respectively.

1

1 15. (Rejected) The electronic circuit of claim 1, wherein the selector includes an OR
2 merger circuit to receive the output of the first combinatorial logical circuit and to
3 receive the output of the second combinatorial logic circuit, and to output, as the
4 selected output, a logical OR of the output of the first combinatorial logical circuit and
5 the output of the second combinatorial logic circuit.

1

1 16. (Rejected) A method of processing cryptographic data, comprising:
2 generating a mode signal having one of a given plurality of states;

3 receiving a given input data and generating a cryptographic processed data
4 output, said generating including:

5 generating a first input data, wherein the first input data is a selected one
6 of a mask of the given input data and a not mask of the given data, the selection
7 based on the state of the mode signal;

8 generating a second input data, wherein the second input data is the other
9 of the mask of the given input data and the not mask of the given data,

10 performing a first set of logical operations on the first input data to
11 generate a first output data, the first set of logical operations embodying a given
12 input-output function,

13 performing a second set of logical operations on the second input data to
14 generate a second output data, the second set of logical operations being
15 different than the first set of logical operations and the second set of logical
16 operations embodying the same given input-output function, and
17 merging the first output data and the second output data to generate the
18 cryptographic data output;

19 repeating said generating a mode signal to have a different one of the given
20 plurality of states; and

21 repeating said receiving a given input data and generating a cryptographic
22 processed data output.

1 17. (Objected) The electronic circuit of claim 1,

2 wherein the first combinatorial logical circuit comprises a first configuration of
3 logical gates receiving a given power supply current, having an input, arranged to
4 receive an input data A at said input and generate a cryptographic output data = $f(A)$, f
5 being a given function, by performing $f(A)$ as a first set of logical operations on said first
6 configuration of logical gates,

7 wherein said first configuration and said first set of logical operations are
8 configured to generate a first power consumption profile when performing $f(A)$, and

9 wherein the first combinatorial logical circuit comprises a second configuration of
10 logical gates receiving a given power supply current, having an input, arranged to
11 receive an input data A at said input and generate a cryptographic output data = $g(A)$,
12 g being a given function, wherein $g(A) = f(A)$ for all A in a given range of A , by
13 performing $g(A)$ as a second set of logical operations on said second configuration of
14 logical gates, and

15 wherein said second configuration and said second set of logical operations are
16 configured to generate a second power consumption profile when performing $g(A)$
17 different from the first power consumption profile in performing $f(A)$.

1
1 18. (Objected) The electronic circuit of claim 17,
2 wherein the selector is configured for receiving a given input data A and

3 dynamically selecting from among the first combinatorial logical circuit for performing
4 said $f(A)$ = the cryptographic output data and the second combinatorial logical circuit
5 for performing said $g(A)$ = the cryptographic output data and producing a selected
6 cryptographic output data as a selected one of either of $f(A)$ and $g(A)$, based said dynamic
7 selecting.

1
1 19. (Objected) The electronic circuit of claim 1,
2 wherein the first combinatorial logical circuit comprises a first configuration of
3 AND, OR and NOT logical gates receiving a given power supply current, having an
4 input, arranged to receive an input data A at said input and generate a cryptographic
5 output data = $f(A)$, f being a given function, by performing $f(A)$ as a first set of logical
6 AND, OR and NOT operations on said first configuration of AND, OR and NOT logical
7 gates, and

8 wherein the second combinatorial logical circuit comprises a second configuration
9 of AND, OR and NOT logical gates receiving a given power supply current, having an
10 input, arranged to receive an input data A at said input and generate a cryptographic
11 output data = $g(A)$, g being a given function, wherein $g(A) = f(A)$ for all A in a given
12 range of A , by performing $g(A)$ as a second set of logical AND, OR and NOT operations
13 on said second configuration of AND, OR and NOT logical gates, and

14 wherein said second configuration and said second set of logical AND, OR and

15 NOT operations are different from said first configuration and said first set of logical
16 AND, OR and NOT operations.

1

1 20. (Objected) The electronic circuit of claim 19,

2 wherein the selector is configured to receive the given input data A and
3 dynamically select from among the first combinatorial logical circuit for performing
4 said $f(A)$ = the cryptographic output data and the second combinatorial logical circuit
5 for performing said $g(A)$ = the cryptographic output data and to produce a selected
6 cryptographic output data as a selected one of $f(A)$ and $g(A)$, based on said dynamic
7 selecting.

1

1 21. (Objected) The electronic circuit of claim 20,

2 wherein the first combinatorial logical circuit comprises a first configuration of
3 AND, OR and NOT logical gates receiving a given power supply current, having an
4 input, arranged to receive an input data A at said input and generate a cryptographic
5 output data = $f(A)$, f being a given function, by performing $f(A)$ as a first set of logical
6 AND, OR and NOT operations on said first configuration of AND, OR and NOT logical
7 gates, wherein said first configuration and said first set of logical AND, OR and NOT
8 operations are configured to generate a first power consumption profile when
9 performing $f(A)$,

10 and

11 wherein the second combinatorial logical circuit comprises a second
12 combinatorial logical circuit comprising a second configuration of AND, OR and NOT
13 logical gates receiving a given power supply current, having an input, arranged to
14 receive an input data A at said input and generate a cryptographic output data = $g(A)$,
15 g being a given function, wherein $g(A) = f(A)$ for all A in a given range of A , by
16 performing $g(A)$ as a second set of logical AND, OR and NOT operations on said second
17 configuration of AND, OR and NOT logical gates, and

18 wherein said second configuration and said second set of logical AND, OR and
19 NOT operations are different from said first configuration and said first set of logical
20 AND, OR and NOT operations and wherein said second configuration and said second
21 set of logical AND, OR and NOT operations are configured to generate a second power
22 consumption profile when performing $g(A)$ and, wherein, for a given A , the first power
23 consumption profile in performing $f(A)$ is different from the second power consumption
24 profile in performing $g(A)$.

1

1 22. (Objected) The electronic circuit of claim 2,

2 wherein the first combinatorial logical circuit comprises a first configuration of
3 AND, OR and NOT logical gates receiving a given power supply current, having an
4 input, arranged to receive an input data A at said input and generate a cryptographic

5 output data = $f(A)$, f being a given function, by performing $f(A)$ as a first set of logical
6 AND, OR and NOT operations on said first configuration of AND, OR and NOT logical
7 gates, wherein said first configuration and said first set of logical AND, OR and NOT
8 operations are configured to generate a first power consumption profile when
9 performing $f(A)$,

10 wherein the second combinatorial logical circuit comprises a second
11 combinatorial logical circuit comprising a second configuration of AND, OR and NOT
12 logical gates receiving a given power supply current, having an input, arranged to
13 receive an input data A at said input and generate a cryptographic output data = $g(A)$,
14 g being a given function, wherein $g(A) = f(A)$ for all A in a given range of A , by
15 performing $g(A)$ as a second set of logical AND, OR and NOT operations on said second
16 configuration of AND, OR and NOT logical gates, and

17 wherein said second configuration and said second set of logical AND, OR and
18 NOT operations are different from said first configuration and said first set of logical
19 AND, OR and NOT operations,

20 wherein said second configuration and said second set of logical AND, OR and
21 NOT operations are configured to generate a second power consumption profile when
22 performing $g(A)$ and, wherein, for a given A , the first power consumption profile in
23 performing $f(A)$ is different from the second power consumption profile in performing
24 $g(A)$,

25 wherein the third combinatorial logical circuit comprises a third configuration of
26 AND, OR and NOT logical gates receiving a given power supply current, having an
27 input, arranged to receive an input data *B* at said input and generate a cryptographic
28 output data = *f1*(*B*), *f1* being a given function, by performing *f1* (*B*) as a third set of
29 logical AND, OR and NOT operations on said third configuration of AND, OR and NOT
30 logical gates,

31 wherein said third configuration and said third set of logical AND, OR and NOT
32 operations are configured to generate a third power consumption profile when
33 performing *f1*(*A*), and

34 a fourth combinatorial logical circuit comprising a fourth configuration of AND,
35 OR and NOT logical gates receiving a given power supply current, having an input,
36 arranged to receive an input data *B* at said input and generate a cryptographic output
37 data ,

38 wherein said cryptographic output data = *g1*(*B*), *g1* being a given function,
39 wherein *g1*(*B*) = *f1*(*B*) for all *B* in a given range of *B*, by performing *g1*(*B*) as a fourth set
40 of logical AND, OR and NOT operations on said fourth configuration of AND, OR and
41 NOT logical gates,

42 wherein said fourth configuration and said fourth set of logical AND, OR and
43 NOT operations are different from said third configuration and said third set of logical
44 AND, OR and NOT operations,

45 wherein said fourth configuration and said fourth set of logical AND, OR and
46 NOT operations are configured to generate a fourth power consumption profile when
47 performing $gI(B)$ and,

48 wherein, for a given B, the third power consumption profile in performing $fI(B)$ is
49 different from the fourth power consumption profile in performing $gI(B)$.

IX. EVIDENCE APPENDIX

A copy of the following evidence 1) entered by the Examiner, including a statement setting forth where in the record the evidence was entered by the Examiner, 2) relied upon by the Appellant in the appeal, and/or 3) relied upon by the Examiner as to the grounds of rejection to be reviewed on appeal, is attached:

NONE

X. RELATED PROCEEDINGS APPENDIX

Copies of relevant decisions in prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal are attached:

NONE